Characterizing Abelian Varieties by the Reductions of the Mordell-Weil Group

Chris Hall and Antonella Perucca

Abstract

Let A be an abelian variety defined over a number field K. If $\mathfrak{p}$ is a prime of K of good reduction for A, let $A(K)_\mathfrak{p}$ denote the image of the Mordell-Weil group via reduction modulo $\mathfrak{p}$. We prove in particular that the size of $A(K)_\mathfrak{p}$, by varying $\mathfrak{p}$, encodes enough information to determine the K-isogeny class of A, provided that the following necessary condition is satisfied: $B(K)$ has positive rank for every non-trivial abelian subvariety B of A. This is the analogue to a result by Faltings of 1983 considering instead the Hasse-Weil zeta function of the special fibers $A_\mathfrak{p}$.

1 Introduction

Let K be a number field and A, A' be abelian varieties over K. A well-known result of Faltings ([2]) implies that A, A' are K-isogenous if and only if they have the same L-series. More precisely, if $S = S(A, A')$ is the set of finite primes $\mathfrak{p} \subseteq K$ of common good reduction for A, A' and if $S' \subseteq S$ has density one, then A, A' are K-isogenous if and only if, for every $\mathfrak{p} \in S'$, the special fibers $A_\mathfrak{p}, A'_\mathfrak{p}$ have the same Hasse–Weil zeta function. The L-series of A is determined, in part, by the function $\nu : \mathfrak{p} \in S \mapsto \#A(k_\mathfrak{p})$, and in this paper we consider other functions which one can use to characterize K-isogeny.

Let $\Gamma \subseteq A(K), \Gamma' \subseteq A'(K)$ be subgroups, and for each $\mathfrak{p} \in S$, let $\Gamma_\mathfrak{p} \subseteq A(k_\mathfrak{p})$, $\Gamma'_\mathfrak{p} \subseteq A'(k_\mathfrak{p})$ be the respective reductions. For each prime ℓ, we consider the composition of the functions $\mathfrak{p} \mapsto \Gamma_\mathfrak{p}$ and $\mathfrak{p} \mapsto \Gamma'_\mathfrak{p}$ with the function which sends a finite group G to the ℓ-adic valuation of the order, exponent, or radical (of the order) of G and which we denote $\mathrm{ord}_\ell(G)$, $\exp_\ell(G)$, and $\mathrm{rad}_\ell(G)$ respectively. Rather than consider these functions for arbitrary A, A' and Γ, Γ', we place conditions on A and Γ, Γ'.

We say A is *square free* if the only abelian variety B for which there exists a K-homomorphism $B^2 \to A$ with finite kernel is $B = 0$. We say Γ (resp. Γ') is a *submodule* if and only if it is an $\mathrm{End}_K(A)$-submodule (resp. $\mathrm{End}_K(A')$-submodule), and we say Γ is *dense* if and only if $\pi(\Gamma) \neq \{0\}$ for every $\pi \neq 0 \in \mathrm{End}_K(A)$.

Theorem 1.1. *Let A, A' be abelian varieties and $S' \subseteq S(A, A')$ have density one, and suppose $\Gamma \subseteq A(K)$, $\Gamma' \subseteq A'(K)$ are submodules. If Γ is dense and if $\ell \gg 0$, then the following are equivalent:*

1. *there exists* $\phi \in \mathrm{Hom}_K(A, A')$ *such that* $\ker(\phi)$ *and* $[\phi(\Gamma) : \phi(\Gamma) \cap \Gamma']$ *are finite;*

2. $\mathrm{ord}_\ell(\Gamma_\mathfrak{p}) \leq \mathrm{ord}_\ell(\Gamma'_\mathfrak{p})$ *for every* $\mathfrak{p} \in S'$.

If moreover A *is square free and if* $\ell \gg 0$*, then these are equivalent to the following:*

3. $\exp_\ell(\Gamma_\mathfrak{p}) \leq \exp_\ell(\Gamma'_\mathfrak{p})$ *for every* $\mathfrak{p} \in S'$*;*

4. $\mathrm{rad}_\ell(\Gamma_\mathfrak{p}) \leq \mathrm{rad}_\ell(\Gamma'_\mathfrak{p})$ *for every* $\mathfrak{p} \in S'$.

Clearly if Γ is $\{0\}$ or even finite, then conditions 2,3,4 hold *regardless* of what A, A', Γ' are. In order to avoid pathologies like this assume Γ is dense, or equivalently, the intersection of Γ with each non-trivial abelian subvariety $B \subseteq A$ is infinite. Also, for any finite group G, $\exp_\ell(G \times G) = \exp_\ell(G)$ and $\mathrm{rad}_\ell(G \times G) = \mathrm{rad}_\ell(G)$, hence the reason we must suppose A is square free in 3 and 4.

As one might expect, Kummer theory lies at the core of our proof of the theorem, and the subgroups which give the cleanest statements, especially when characterizing when distinct subgroups are 'independent,' are submodules. The basic strategy we employ to prove an equivalence such as $1 \Leftrightarrow 2$ is to prove two implications: $1 \Rightarrow 2$ and $\neg 1 \Rightarrow \neg 2$. The first implication is straightforward. A crucial notion which appears in the second implication is of 'almost free' points, and we develop this notion in section 3. Prior to this we give some preliminary results in section 2, and finally, we prove theorem 1.1 in section 4.

Note, the Mordell-Weil group of an abelian variety is a dense submodule if and only if the Mordell-Weil group of every abelian subvariety is infinite. Then we have the following:

Corollary 1.2. *Let* A, A' *be abelian varieties and* $S' \subseteq S(A, A')$ *have density one, and suppose* $B(K)$ *is infinite for every non-trivial abelian subvariety* $B \subseteq A$*. For every fixed* $\ell \gg 0$*, the* K*-isogeny class of* A *is determined by the function* $\mathfrak{p} \in S' \mapsto \#A(K)_\mathfrak{p}$*. If moreover* A *is square-free and* $\ell \gg 0$*, then the* K*-isogeny class of* A *is determined by the function* $\mathfrak{p} \in S' \mapsto \mathrm{rad}_\ell A(K)_\mathfrak{p}$*, hence a fortiori by the function* $\mathfrak{p} \in S' \mapsto \exp_\ell A(K)_\mathfrak{p}$.

If $A(K)$ and $A'(K)$ are free of rank 1 and the functions $\mathfrak{p} \mapsto \exp_\ell(A(K)_\mathfrak{p})$ and $\mathfrak{p} \mapsto \exp_\ell(A'(K)_\mathfrak{p})$ are considered, the above result relates to the so-called support problem (cf. [1, thm. 1.2]). Note that there exist pairs of elliptic curves over a number field K which are not K-isomorphic but such that for every prime number ℓ there is a K-isogeny between them of degree coprime to ℓ (cf. [6, sec. 12]). This implies that it is not possible to characterize the K-isomorphism class of A by knowing the order and the exponent of $A(K)_\mathfrak{p}$ for $\mathfrak{p}$ varying in a set of density 1.

1.1 Notation

Unless explicitly stated otherwise, we assume all abelian varieties, subvarieties, homomorphisms, etc. are defined over K. Given an abelian variety A, we denote by $S(A)$ the set of finite primes $\mathfrak{p} \subset K$ of good reduction for A, and we write $k_\mathfrak{p}$ for the residue field and

$A(k_\mathfrak{p})$ for the group of $k_\mathfrak{p}$-rational points. By the density of a subset $S' \subseteq S(A)$ we mean the Dirichlet density. We also write $\mathrm{E}(A)$ for the ring $\mathrm{End}_K(A)$, and given a second abelian variety B, we write $\mathrm{H}(A,B)$ for $\mathrm{Hom}_K(A,B)$.

Given $\mathfrak{p} \in S(A)$ and a subgroup $\Gamma \subseteq A(K)$, we write $\Gamma_\mathfrak{p} \subseteq A(k_\mathfrak{p})$ for the reduction of Γ modulo $\mathfrak{p}$. Moreover, for each rational prime ℓ, we define the following functions on $S(A)$:

$$\nu_{\ell,\Gamma} : \mathfrak{p} \mapsto \mathrm{ord}_\ell(\Gamma_\mathfrak{p}), \quad \varepsilon_{\ell,\Gamma} : \mathfrak{p} \mapsto \exp_\ell(\Gamma_\mathfrak{p}), \quad \rho_{\ell,\Gamma} : \mathfrak{p} \mapsto \mathrm{rad}_\ell(\Gamma_\mathfrak{p}).$$

They respectively express the ℓ-adic valuations of the size, the exponent, and the radical of the size of $\Gamma_\mathfrak{p}$.

2 Preliminaries

In this section we develop results we need for the proof of theorem 1.1.

2.1 Homomorphisms

Let A, B be abelian varieties. We make frequent use of the following lemma:

Lemma 2.1. *Let $\phi \in \mathrm{H}(A,B)$ and let $B' \subseteq B$ be the image of ϕ. There exist $A' \subseteq A$ and $\psi \in \mathrm{H}(B,A')$ such that $B' + \ker(\psi) = B$ and such that the restrictions $\psi\,|_{B'}$ and $\phi\,|_{A'}$ are isogenies between A' and B' and satisfy $\phi\psi\,|_{B'} = [m]_{B'}$, $\psi\phi\,|_{A'} = [m]_{A'}$ for some $m \geq 1$.*

Proof. If $A'' \subseteq A$ is the kernel of ϕ, then the Poincaré Reducibility Theorem implies there exists $A' \subseteq A$ such that $A' + A'' = A$ and $A' \cap A''$ is finite. Similarly, there exists $B'' \subseteq B$ such that $B' + B'' = B$ and $n = \#(B' \cap B'')$ is finite, and then the restriction $\phi|_{A'} : A' \to B'$ is isogeny and there exists $\hat{\phi} : B' \to A'$ and $m' \geq 1$ such that $\hat{\phi}\phi|_{A'} = [m']_{A'}$ and $\phi\hat{\phi} = [m']_{B'}$ (cf. [3, lem. A.5.1.5]). The restriction of $n\hat{\phi}$ to $B' \cap B''$ is trivial, hence $n\hat{\phi}$ extends (uniquely) to a homomorphism $\psi : B \to A'$ such that $B'' \subseteq \ker(\psi)$ and $\psi\phi|_{A'} = [m]_{A'}$, $\phi\psi|_{B'} = [m]_{B'}$ for $m = m'n$. □

Corollary 2.2. $\mathrm{H}(A,B) = \{0\}$ *if and only if* $\mathrm{H}(B,A) = \{0\}$.

Proof. The statement is symmetric in A, B, so it suffices to suppose $\mathrm{H}(A,B) \neq \{0\}$ and show that $\mathrm{H}(B,A) \neq \{0\}$. If $\phi \neq 0 \in \mathrm{H}(A,B)$ and if $\psi \in \mathrm{H}(B,A)$ and $m \geq 1$ are as in lemma 2.1, then $\psi\phi \neq 0$, so $\psi \neq 0$ and hence $\mathrm{H}(B,A) \neq \{0\}$. □

2.2 Images of Submodules

Let $\Gamma \subseteq A(K)$ be a submodule and $\phi \in \mathrm{H}(A,B)$. We write $\phi_*(\Gamma) \subseteq B(K)$ for the submodule generated by $\phi(\Gamma)$.

Lemma 2.3. *Suppose $\hat{\phi} \in \mathrm{H}(B,A)$ and $m \geq 1$ satisfy $\hat{\phi}\phi = [m]_A$. If ϕ is an isogeny, then the index of $\phi(\Gamma)$ in $\phi_*(\Gamma)$ divides m.*

Proof. Suppose ϕ is an isogeny and thus $\phi\hat{\phi} = [m]_B$. If $P_1, \ldots, P_r \in \Gamma$ and if $\phi_1, \ldots, \phi_r \in \mathrm{E}(B)$, then $Q = \Sigma_i \phi_i \phi(P_i)$ satisfies $mQ = \phi(\Sigma_i \hat{\phi}\phi_i \phi(P_i)) \in \phi(\Gamma)$ and thus $m\phi_*(\Gamma) \subseteq \phi(\Gamma)$. □

Remark 2.4. *If $Q_1, \ldots, Q_r \in \phi(G)$ and if $\phi_1, \ldots, \phi_r \in \mathrm{E}(B)$, then for $Q = \Sigma_i \phi_i(Q)$ and $\mathfrak{p} \in S(A) \cap S(B)$, the exponent of the reduction $Q_\mathfrak{p}$ divides the least-common multiple of the exponents of the reductions $Q_{i,\mathfrak{p}}$, thus $\exp_\ell(\phi_*(\Gamma)_\mathfrak{p}) = \exp_\ell(\phi(\Gamma)_\mathfrak{p})$ for every ℓ.*

2.3 Dense Submodules

Recall that a submodule $\Gamma \subseteq A(K)$ is *dense* if and only if it satisfies condition 3 in the following lemma:

Lemma 2.5. *If $\Gamma \subseteq A(K)$ is a submodule, then the following are equivalent:*

1. *$\phi(\Gamma) \neq \{0\}$ for every abelian variety B and $\phi \neq 0 \in \mathrm{H}(A, B)$;*
2. *$\phi'(\Gamma) \neq \{0\}$ for every simple abelian variety B' and $\phi' \neq 0 \in \mathrm{H}(A, B')$;*
3. *$\pi(\Gamma) \neq \{0\}$ for every $\pi \neq 0 \in \mathrm{E}(A)$.*

Proof. Clearly $1 \Rightarrow 2, 3$. Suppose B is an abelian variety and $\phi \neq 0 \in \mathrm{H}(A, B)$, and let $B' \subseteq B$ be a non-zero simple abelian subvariety. If $B' \subseteq \phi(A)$ and if $\pi' \in \mathrm{H}(B, B')$ and $m \geq 1$ satisfy $\pi'|_{B'} = [m]_{B'}$, then $\phi' = \pi'\phi \neq 0 \in \mathrm{H}(A, B')$ since the composition of ϕ' with inclusion $B' \subseteq B$ equals $m\phi$. In particular, if $\phi'(\Gamma) \neq \{0\}$, then $\phi(\Gamma) \neq \{0\}$, thus $2 \Rightarrow 1$. Similarly, if $\psi \in \mathrm{H}(B, A)$ and $m \geq 1$ satisfy $\phi\psi|_{\phi(A)} = [m]_{\phi(A)}$, then $\pi = \psi\phi \neq 0 \in \mathrm{E}(A)$ since $\phi\pi = m\phi \neq 0$, and thus $3 \Rightarrow 1$. □

Remark 2.6. *If $\Gamma \subseteq A(K)$ is a finite submodule, then it is not dense, so a dense submodule is infinite. Conversely, if A is simple and if $\Gamma \subseteq A(K)$ is an infinite submodule, then Γ is dense.*

2.4 Isogeny Invariance

Let $\Gamma \subseteq A(K)$, $\Gamma' \subseteq A'(K)$ be submodules. The following lemma shows that condition 1 of theorem 1.1 is isogeny invariant:

Lemma 2.7. *Suppose that $\iota \in \mathrm{H}(A, B)$, $\iota' \in \mathrm{H}(A', B')$ are isogenies. Then there exist $\hat{\iota} \in \mathrm{H}(B, A)$, $\hat{\iota}' \in \mathrm{H}(B', A')$ and $m, m' \geq 1$ satisfying $\hat{\iota}\iota = [m]_A$ and $\hat{\iota}'\iota' = [m']_{A'}$, and the following are equivalent:*

1. *$\exists\, \phi \in \mathrm{H}(A, A')$ such that $\ker[\phi]$ and $[\phi(m\Gamma) : \phi(m\Gamma) \cap m'\Gamma']$ are finite;*
2. *$\exists\, \phi \in \mathrm{H}(A, A')$ such that $\ker[\phi]$ and $[\phi(\Gamma) : \phi(\Gamma) \cap \Gamma']$ are finite;*
3. *$\exists\, \phi' \in \mathrm{H}(B, B')$ such that $\ker[\phi']$ and $[\phi'\iota(\Gamma) : \phi'\iota(\Gamma) \cap \iota'(\Gamma')]$ are finite;*

4. $\exists\, \phi' \in \mathrm{H}(B, B')$ *such that* $\ker[\phi']$ *and* $[\phi'(\iota_*(\Gamma)) : \phi'(\iota_*(\Gamma)) \cap \iota'_*(\Gamma')]$ *are finite.*

Proof. Clearly $1 \Leftrightarrow 2$. By lemma 2.3, $[\iota_*(\Gamma) : \iota(\Gamma)]$ and $[\iota'_*(\Gamma') : \iota'(\Gamma')]$ are finite, and thus $3 \Leftrightarrow 4$. Let $\hat{\iota} : B \to A$ and $m \geq 1$ satisfy $\hat{\iota}\iota = [m]_A$, and let $\hat{\iota}' : B' \to A'$ and $m' \geq 1$ be defined similarly (see lemma 2.1). If $\phi \in \mathrm{H}(A, A')$ has finite kernel, then $\phi' = \iota'\phi\hat{\iota}$ lies in $\mathrm{H}(B, B')$ and also has finite kernel. If moreover $\phi(\Gamma) \cap \Gamma'$ has finite index in $\phi(\Gamma)$, then $m\phi(\Gamma) \cap \Gamma'$ has finite index in $m\phi(\Gamma) = \phi\hat{\iota}(\iota(\Gamma))$ and thus $\iota'\phi\hat{\iota}(\iota(\Gamma)) \cap \iota'(\Gamma')$ has finite index in $\iota'\phi\hat{\iota}(\iota(\Gamma)) = \phi'(\iota(\Gamma))$. That is, $2 \Rightarrow 3$, and a similar argument shows $3 \Rightarrow 1$ since $\hat{\iota}\iota(\Gamma) = m\Gamma$ and $\hat{\iota}'\iota'(\Gamma') = m'\Gamma'$. □

The following lemma shows that, in theorem 1.1, $1 \Rightarrow 2$ and moreover $1 \Rightarrow 3, 4$ if A is square free:

Lemma 2.8. *Let* $\phi \in \mathrm{H}(A, A')$. *If* $\ker(\phi)$ *and* $i = [\phi(\Gamma) : \phi(\Gamma) \cap \Gamma']$ *are finite, then the following holds for* $\ell \nmid i \cdot \deg(\phi)$*:*

$$\nu_{\ell,\Gamma}(\mathfrak{p}) \leq \nu_{\ell,\Gamma'}(\mathfrak{p}), \quad \varepsilon_{\ell,\Gamma}(\mathfrak{p}) \leq \varepsilon_{\ell,\Gamma'}(\mathfrak{p}), \quad \rho_{\ell,\Gamma}(\mathfrak{p}) \leq \rho_{\ell,\Gamma'}(\mathfrak{p}) \qquad \forall \mathfrak{p} \in S(A) \cap S(A').$$

Proof. Let $\mathfrak{p} \in S(A) \cap S(A')$. If $\ell \nmid \deg(\phi)$, then ϕ induces an isomorphism of the ℓ-parts of $\Gamma_{\mathfrak{p}}$ and $\phi(\Gamma)_{\mathfrak{p}}$, thus $\nu_{\ell,\Gamma}(\mathfrak{p}) = \nu_{\ell,\phi(\Gamma)}(\mathfrak{p})$. Moreover, if $\ell \nmid i$, then the ℓ-parts of $\phi(\Gamma)_{\mathfrak{p}} \cap \Gamma'_{\mathfrak{p}}$ and $\phi(\Gamma)_{\mathfrak{p}}$ coincide, so $\nu_{\ell,\phi(\Gamma)}(\mathfrak{p}) = \nu_{\ell,\phi(\Gamma)\cap\Gamma'}(\mathfrak{p}) \leq \nu_{\ell,\Gamma'}(\mathfrak{p})$. Thus the first inequality holds, and a similar argument yields the other inequalities. □

Corollary 2.9. *Suppose* $\Gamma \subseteq A(K)$, $\Gamma' \subseteq A'(K)$ *are submodules,* $\iota \in \mathrm{H}(A, B)$, $\iota' \in \mathrm{H}(A', B')$ *are isogenies, and* $d \geq 1$ *is an integer. Theorem 1.1 holds for* A, A', Γ, Γ' *and* $\ell \nmid d$ *if and only if it holds for* $B, B', \iota_*(\Gamma), \iota'_*(\Gamma)$ *and* $\ell \nmid d \cdot \deg(\iota) \cdot \deg(\iota')$.

Proof. The equivalences of lemma 2.7 implies that condition 1 of theorem 1.1 holds for A, A', Γ, Γ' if and only if it holds for $B, B', \iota_*(\Gamma), \iota_*(\Gamma')$. For the remaining three conditions of theorem 1.1, we observe that, for each $\ell \nmid \deg(\iota)$, we have $\nu_{\ell,\Gamma} = \nu_{\ell,\iota_*(\Gamma)}$, $\rho_{\ell,\Gamma} = \rho_{\ell,\iota_*(\Gamma)}$, and $\varepsilon_{\ell,\Gamma} = \varepsilon_{\ell,\iota_*(\Gamma)}$ on $S(A) \cap S(A')$. Similarly, on $S(A) \cap S(A')$ we have $\nu_{\ell,\Gamma'} = \nu_{\ell,\iota'_*(\Gamma')}$, $\rho_{\ell,\Gamma'} = \rho_{\ell,\iota'_*(\Gamma')}$, and $\varepsilon_{\ell,\Gamma'} = \varepsilon_{\ell,\iota'_*(\Gamma')}$, for each $\ell \nmid \deg(\iota')$. Thus if $\ell \nmid \deg(\iota) \cdot \det(\iota')$, then each condition of theorem 1.1 holds for both A, A', Γ, Γ' and $B, B', \iota_*(\Gamma), \iota'_*(\Gamma')$ or for neither. □

3 Almost Free Points

Let $A_1, \ldots, A_r$ be abelian varieties. We say $P_1 \in A_1(K), \ldots, P_r \in A_r(K)$ are *almost free* points if and only if they have infinite order and the following implication holds for all i:

$$\Pi_j \phi_j \in \Pi_j \mathrm{H}(A_j, A_i), \quad \Sigma_j \phi_j(P_j) = 0 \quad \Rightarrow \quad \phi_1(P_1) = \cdots = \phi_r(P_r) = 0. \tag{1}$$

Note, if $X, Y \subset A(K)$ are subsets of almost free points and if Γ, Γ' are the respective submodules they generate, then non-zero elements of $\Gamma \cap \Gamma'$ correspond bijectively to violations of (1) for $X \cup Y$ because such elements have (exactly) two representations, one each in elements of X, Y respectively.

Recall that points $P_1, \dots, P_r \in A(K)$ are *independent* (or *free*) if and only if $\Sigma_i \phi_i(P_i) = 0$ for $\phi_i \in \mathrm{E}(A)$ implies $\phi_i = 0$ for all i (cf. [4, def. 3 and rem. 6]). If $P \in A(K)$ is independent, then it is almost free, but the converse does not hold in general. For example, if A_1, A_2 are non-isogenous and simple and if $P_1 \in A_1(K), P_2 \in A_2(K)$ have infinite order, then $P_1, P_2, P_1 + P_2$ are each almost free points of $A = A_1 \times A_2$, but only $P_1 + P_2$ is free.

Lemma 3.1. *Suppose $P_1 \in A_1(K), \dots, P_r \in A_r(K)$ are almost free, and for each i, suppose the Zariski closure $B_i \subseteq A_i$ of P_i is connected. If $B = \Pi_i B_i$, then $P = \Pi_i P_i$ is independent.*

Proof. Suppose $\phi \in \mathrm{E}(B)$. We may write ϕ as an $r \times r$ matrix (ϕ_{ij}) where $\phi_{ij} \in \mathrm{H}(B_i, B_j)$, and thus $\phi(P) = \Pi_j P'_j$ for $P'_j = \Sigma_i \phi_{ij}(P_i)$. We must show that if $\phi(P) = 0$, then $\phi = 0$. If $\phi(P) = 0$, then $P'_j = 0$ for all j, and hence $\phi_{ij}(P_i) = 0$ for all i, j since $P_1, \dots, P_r$ are almost free. Therefore, since P_i is Zariski dense in B_i for every i, we have $\phi_{ij} = 0$ for every i, j, that is, $\phi = 0$. □

The following proposition is a key ingredient in our proof of theorem 1.1:

Proposition 3.2. *Suppose $P_1, \dots, P_r \in A(K)$ and $m_1, \dots, m_r \geq 0$. If $P_1, \dots, P_r$ are almost free, then for every $\ell \gg 0$, the following set has positive density:*

$$S_{\ell,m} := \{\ \mathfrak{p} \in S(A) : \varepsilon_{\ell,P_i}(\mathfrak{p}) = m_i, \forall i\ \}.$$

Proof. Let $A_i \subseteq A$ be the Zariski closure of P_i. Up to replacing P_i by mP_i, for some $m \geq 1$, and excluding ℓ which divide m, we suppose that A_i is connected. Then lemma 3.1 implies $P = \Pi_i P_i$ is independent in $B = \Pi_i A_i$, and thus the proposition follows from [4, prop. 12]). □

If A is simple and if $\phi \neq 0 \in \mathrm{E}(A)$, then the kernel of ϕ is finite and so $\phi(P) \neq 0$ for any non-torsion $P \in A(K)$. Hence if A is simple and if $P \in A(K)$ is almost free, then P is independent. An analogous remark also holds for more points. The following lemma gives a mildly different characterization of almost free points when A is simple:

Lemma 3.3. *Let A be simple and $P_1, \dots, P_r \in A(K)$ be points of infinite order. The following are equivalent:*

1. *$P_1, \dots, P_r$ are almost free;*
2. *if $\phi_1, \dots, \phi_r \in \mathrm{E}(A)$ satisfy $\Sigma_i \phi_i(P_i) = 0$ and if $\phi_1 \in \mathbb{Z}$, then $\{\phi_i(P_i)\} = \{0\}$.*

Proof. It is clear that $1 \Rightarrow 2$ (cf. (1)), so suppose that 2 holds and $\phi_1, \dots, \phi_r \in \mathrm{E}(A)$ satisfy $\Sigma_i \phi_i(P_i) = 0$. If $\phi_1 = 0$, then it lies in $\mathbb{Z}$ and hence 2 implies $\phi_1(P_1) = \cdots = \phi_r(P_r) = 0$. If $\phi_1 \neq 0$, then its kernel is a proper algebraic subgroup of A, hence it must be a finite subgroup, since A is simple, and thus ϕ_1 is an isogeny. Let $\psi : A \to A$ and $m \geq 1$ satisfy $\psi\phi_1 = [m]_A$. Then $\Sigma_i \psi\phi_i(P_i) = 0$ and $\psi\phi_1 = [m]_A \in \mathbb{Z}$, so 2 implies $\{\psi\phi_i(P_i)\}_i = \{0\}$. Therefore $\phi_i(P_i)$ lies in the kernel of ψ for every i, and thus $\{\phi_i(P_i)\}_i = \{0\}$ since the points P_i have infinite order and A is simple. □

If A is simple and if $\Gamma \subseteq A(K)$ is a submodule, then one can repeatedly apply the following corollary in order to find a finite-index free-submodule $\Gamma' \subseteq \Gamma$ and an explicit basis of Γ':

Corollary 3.4. *Suppose A is simple and $P_1, \dots, P_r \in A(K)$ are almost free, and let $\Gamma \subseteq A(K)$ be the submodule they generate. If $Q \in A(K)$ satisfies $nQ \notin \Gamma$ for every $n \geq 1$, then $P_1, \dots, P_r, Q$ are almost free.*

Proof. The points $P_1, \dots, P_r, Q$ satisfy 2 of lemma 3.3 and thus they are almost free. □

Corollary 3.5. *Suppose A is simple and $\Gamma \subseteq A(K)$ is a submodule. If $Q \in A(K)$ satisfies $nQ \notin \Gamma$, for every $n \geq 1$, and if $\phi \in \mathrm{E}(A)$ satisfies $\phi(Q) \in \Gamma$, then $\phi(Q)$ is torsion.*

Proof. Let $\{P_1, \dots, P_r\} \subset \Gamma$ be a maximal subset of almost free points, and let $\Gamma' \subseteq \Gamma$ be the finite-index submodule they generate (cf. cor. 3.4). If $\phi, \phi_1, \dots, \phi_r \in \mathrm{E}(A)$ satisfy $\phi(Q) \in \Gamma$ and $\phi(nQ) + \Sigma_i \phi_i(P_i) = 0$, where $n = [\Gamma : \Gamma']$, then corollary 3.4 implies $\{\phi(nQ), \phi_i(P_i)\}_i = \{0\}$. That is, $\phi(nQ) = 0$ and thus $\phi(Q)$ is torsion of order dividing n. □

For general A, we can repeatedly apply the following lemma to choose a 'quasi-basis' of a submodule, that is, a maximal subset of almost free points which generate a finite-index submodule:

Lemma 3.6. *Let $P_1, \dots, P_r \in A(K)$ be almost free, and suppose the submodule $\Gamma \subseteq A(K)$ they generate is torsion free. If $\Gamma' \subseteq A(K)$ is a submodule such that $\Gamma \cap \Gamma'$ has infinite index in Γ', then there exists $Q \in \Gamma'$ such that $P_1, \dots, P_r, Q$ are almost free and such that the submodule they generate is torsion free.*

Proof. Let $B, B' \subseteq A$ be abelian varieties such that $\mathrm{H}(B, B') = \mathrm{H}(B', B) = \{0\}$ and $B + B' = A$. Let $\hat{\pi} : B \to A$ and $\hat{\pi}' : B' \to A$ be the natural inclusions, and suppose $\pi \in \mathrm{H}(A, B)$, $\pi' \in \mathrm{H}(A, B')$, and $m, m' \geq 1$ satisfy $\pi\hat{\pi} = [m]_B$ and $\pi'\hat{\pi}' = [m']_{B'}$.

Suppose B is minimal with the property that $\pi(\Gamma \cap \Gamma')$ has infinite index in $\pi(\Gamma')$. Thus there is a simple abelian subvariety $C \subseteq B$ and an isogeny $\psi : B \to C^e$ for some $e \geq 1$, and we define $\pi_i : A \to C$ to be the composition of $\psi\pi$ with projection onto the ith factor and let $\hat{\pi}_i : C \to A$ and $m_i \geq 1$ be such that $\pi_i\hat{\pi}_i = [m_i]_C$. We note that $\ker(\pi)$ has finite index in $\cap_i \ker(\hat{\pi}_i\pi_i)$ and that the intersection of either with $\ker(\pi')$ is finite.

Let i be such that $\pi_i(\Gamma \cap \Gamma')$ has infinite index in $\pi_i(\Gamma')$. Therefore there exists $Q' \in \Gamma'$ such that $n\pi_i(Q') \notin \pi_i(\Gamma)$, for every $n \geq 1$, and we let $Q = \hat{\pi}_i(\pi_i(Q'))$. Up to replacing Q' by nQ' for some $n \geq 1$, we suppose without loss of generality that the submodule generated by $P_1, \dots, P_s, Q$ is torsion free.

From the equality $m_i\pi_j(\Gamma) = \pi_i\hat{\pi}_i\pi_j(\Gamma)$ it follows that $[\pi_j(\Gamma) : \pi_i(\Gamma) \cap \pi_j(\Gamma)]$ is finite, for every j, and so we have $n\pi_j(Q) \notin \pi_j(\Gamma)$ for every $n \geq 1$. Moreover, for $\phi \in \mathrm{E}(A)$ and $\phi'_{ij} = \pi_j\phi\hat{\pi}_i \in \mathrm{E}(C)$, we have the identity $\pi_j(\phi(Q)) = \phi'_{ij}\pi_i(Q')$ and thus corollary 3.5

implies $\pi_j\phi(Q) \in \pi_j(\Gamma)$ only if $\pi_j\phi(Q)$ has finite order. Up to replacing Q by nQ, for some $n \geq 1$, we may suppose that $\pi_j\phi(Q) \in \pi_j(\Gamma)$ only if $\pi_j\phi(Q) = 0$.

Let $\phi_1, \ldots, \phi_r, \phi \in \mathrm{E}(A)$, and suppose $\Sigma_j \phi_j(P_j) + \phi(Q) = 0$. Our assumptions on B, B' imply $\mathrm{H}(C, B') = \{0\}$, thus $\pi'\phi\hat{\pi}_i = 0$ and $\pi'\phi(Q) = \pi'\phi\hat{\pi}_i(\pi_i(Q')) = 0$. That is, $\Sigma_j \pi'\phi_j(P_j) = 0$ and hence $\Sigma_j \hat{\pi}'\pi'\phi_j(P_j) = 0$. Since $P_1, \ldots, P_r$ are almost free, $\{\hat{\pi}'\pi'\phi_j(P_j)\}_j = \{0\}$, and thus since $\hat{\pi}' : B' \to A$ is injective, we have $\{\pi'\phi_j(P_j)\}_j = \{0\}$. Therefore $\{\phi_j(P_j), \phi(Q)\}_j$ lies in the kernel of π'. We will show that it also lies in $\cap_k \ker(\hat{\pi}_k\pi_k)$.

By assumption, $\Sigma_j \pi_k\phi_j(P_j) + \pi_k\phi(Q) = 0$ for every k, thus $\pi_k\phi(Q) \in \pi_k(\Gamma)$ and so $\pi_k\phi(Q) = 0$. That is, $\Sigma_j \pi_k\phi_j(P_j) = 0$ for every k, and thus $\Sigma_j \hat{\pi}_k\pi_k\phi_j(P_j) = 0$ and so $\{\hat{\pi}_k\pi_k\phi_j(P_j)\}_j = \{0\}$ since $P_1, \ldots, P_r$ are almost free. Therefore $\{\phi_j(P_j), \phi(Q)\}_j$ lies in the kernel of $\hat{\pi}_k\pi_k$, for every k. That is, $\{\phi_j(P_j), \phi(Q)\}_j$ lies in both $\ker(\pi')$ and $\cap_k \ker(\hat{\pi}_k\pi_k)$ and thus in a finite subgroup of $A(K)$. Since Γ is torsion free and $\phi_j(P_j) \in \Gamma$ for each j, we must have $\{\phi_j(P_j)\}_j = \{0\}$ and thus $\phi(Q) = 0$ as well. That is, $P_1, \ldots, P_r, Q$ are almost free. □

4 Proof of Theorem 1.1

We have already seen that if 1 holds, then 2 holds, and if moreover A is square free, then 3 and 4 hold (see section 2.4). Thus we suppose that 1 fails and show that 2, 3, 4 fail accordingly.

Suppose $P \in A(K)$ and $Q_1, \ldots, Q_r \in A'(K)$ are points, and for each prime ℓ and $m \geq 0$, consider the following set:

$$S_{\ell,m}(P, Q_1, \ldots, Q_r) := \{\ \mathfrak{p} \in S(A) \cap S(A') : \varepsilon_{\ell,P}(\mathfrak{p}) = m,\ \varepsilon_{\ell,Q_i}(\mathfrak{p}) = 0 \text{ for } i = 1, \ldots, r\ \}.$$

The basic strategy underlying our proof is to first make judicious choices of $P, Q_1, \ldots, Q_r$ so that we can analyze the ℓ-parts of $\Gamma_\mathfrak{p}, \Gamma'_\mathfrak{p}$ for $\ell \gg 0$ and varying $\mathfrak{p}$. In particular, we will show these sets usually have positive density and deduce that 2 fails for $\ell \gg 0$, and moreover, that 3 and 4 fail when A is square free and $\ell \gg 0$.

Let B' be an abelian variety such that A and A' each have some abelian subvariety isogenous to B', and we suppose that B' has maximal dimension. Then for some abelian subvarieties $B \subseteq A$, $B'' \subseteq A'$ we have that A, A' are respectively isogenous to $B \times B'$, $B' \times B''$ so, by corollary 2.9, we may assume that $A = B \times B'$, $A' = B' \times B''$. We may also assume $\phi \in H(A, A')$ is the composition of the projection on B' and the inclusion $B' \subseteq A'$.

Lemma 4.1. *We have* $\mathrm{H}(B, B'') = \mathrm{H}(B'', B) = \{0\}$.

Proof. Suppose $\psi \neq 0 \in \mathrm{H}(B, B'')$, and let $\pi : A \to B$ be projection. Up to composing with the natural embedding $B'' \to A'$, we can consider the homomorphism $\phi' = \phi + \psi\pi \in \mathrm{H}(A, A')$, and let $C \subseteq A$ be its kernel. The kernel of ϕ is $B = B \times \{0\} \subseteq A$, and $B' = \{0\} \times B' \subseteq A$ satisfies $B \cap B' = \{0\}$, thus the restriction of ϕ' to $B' \subseteq A$, which is simply ϕ, is injective. The image of ϕ' contains the images of ϕ and ψ, thus it is

strictly larger, so $\dim(\ker(\phi')) = \dim(C) < \dim(\ker(\phi))$. That is, if $\mathrm{H}(B, B'')$ is non trivial, then $\dim(B')$ is not maximal by lemma 2.1. Finally, $\mathrm{H}(B, B'') = \{0\}$ if and only if $\mathrm{H}(B'', B) = \{0\}$ by corollary 2.2. □

Corollary 4.2. *Suppose $P \in B(K)$, and let $\Gamma_0 \subseteq A(K)$ be the submodule it generates. Then $\phi(\Gamma_0) = \{\psi(P) : \psi \in \mathrm{H}(B, A')\}$.*

Proof. Let $\alpha \in \mathrm{E}(A)$ and $\alpha(P) \in \Gamma_0$. Lemma 4.1 implies $\mathrm{H}(B, B'') = \{0\}$ and thus $\phi\alpha(P) = \psi(P)$ for some $\psi \in \mathrm{H}(B, B')$. Conversely, if $\psi \in \mathrm{H}(B, A')$ and if $\pi'' : A' \to B''$ is projection, then $\pi''\psi = 0 \in \mathrm{H}(B, B'')$ and thus ψ factors through the natural embedding $B' \to A'$. In particular, if we compose with the natural embedding $B' \to A$, then the endomorphism $\alpha \in \mathrm{E}(A)$ such that $\alpha|_B = \psi$ and $\alpha|_{B'} = 0$ satisfies $\phi(\alpha(P)) = \psi(P)$ and thus $\psi(P) \in \phi(\Gamma_0)$. □

The following lemma allows us to reduce to the case $B = 0$:

Lemma 4.3. *Suppose that condition 1 in theorem 1.1 fails. If $B' \neq A$ then 2 fails. Moreover, if A is square free, then 3 and 4 also fail.*

Proof. Suppose that $B \neq 0$. If $\pi : A \to B$ is projection, then $\pi(\Gamma) \subseteq B(K)$ is infinite since Γ is dense (see lemma 2.5), so let $P \in \pi(\Gamma)$ have infinite order and let $\Gamma_0 \subseteq \Gamma$ be the submodule it generates. Lemma 4.1 implies $\mathrm{H}(B, B'') = \{0\}$ and thus $\psi(B) \subseteq B'$ for every $\psi \in \mathrm{H}(B, A')$. Thus up to replacing P by nP with n the size of the torsion subgroup of $B'(K)$, we suppose without loss of generality that, for every $\psi \in \mathrm{H}(B, A')$, either $\psi(P) = 0$ or $\psi(P)$ has infinite order.

Let $\{R_1, \dots, R_s\} \subset (\phi(\Gamma_0) \cap \Gamma')$ and $\{Q_1, \dots, Q_r, R_1, \dots, R_s\} \subseteq \Gamma'$ be maximal subsets of almost free points, and let $\Gamma'_0 \subseteq \Gamma'$ be the submodule generated by $Q_1, \dots, Q_r$ and $\Gamma'_1 \subseteq \Gamma'$ be the submodule generated by $R_1, \dots, R_r$. Up to replacing each Q_i by nQ_i with n the size of the torsion subgroup of $B(K)$, we suppose without loss of generality that, for every i and $\psi_i \in \mathrm{H}(A', B)$, either $\psi_i(Q_i) = 0$ or $\psi_i(Q_i)$ has infinite order. Since a maximal subset of almost free points generates a finite index submodule by lemma 3.6, we may suppose that ℓ is coprime with the index of the above submodules. If $\mathfrak{p} \in S_{\ell,m}(P, Q_1, \dots, Q_r)$, then the ℓ-part of $\Gamma'_{\mathfrak{p}}$ lies in that of $(\phi(\Gamma_0) \cap \Gamma')_{\mathfrak{p}}$ and thus

$$\mathrm{ord}_\ell(\Gamma'_{\mathfrak{p}}) \leq \mathrm{ord}_\ell(\Gamma_{\mathfrak{p}}) - \mathrm{ord}_\ell(\Gamma_{\mathfrak{p}} \cap B(K)_{\mathfrak{p}}) \leq \mathrm{ord}_\ell(\Gamma_{\mathfrak{p}}) - m\,.$$

If moreover A is square free, then $\mathrm{H}(B, B') = \{0\}$ and so $\mathrm{H}(B, A') = \{0\}$, thus corollary 4.2 implies $\phi(\Gamma_0) = \{0\}$ and $\varepsilon_{\ell,\Gamma'}(\mathfrak{p}) = 0$.

If $S_{\ell,m}(P, Q_1, \dots, Q_r)$ has positive density for every $m \geq 0$, then $\nu_{\ell,\Gamma}(\mathfrak{p}) - \nu_{\ell,\Gamma'}(\mathfrak{p})$ can be made arbitrarily large on a positive density set, thus 2 fails. If moreover A is square free, then for every $m \geq 0$, the identities $\varepsilon_{\ell,\Gamma}(\mathfrak{p}) \geq m$ and $\varepsilon_{\ell,\Gamma'}(\mathfrak{p}) = 0$ hold on a positive density set, thus 3 and 4 fail. To complete the proof it suffices to show that $P, Q_1, \dots, Q_r$ are almost free because then proposition 3.2 implies that $S_{\ell,m}(P, Q_1, \dots, Q_r)$ has positive density for every $\ell \gg 0$ and $m \geq 0$.

The intersection of Γ_1' and Γ_0' is trivial since $Q_1, \dots, Q_r, R_1, \dots, R_s$ are almost free, thus $\phi(\Gamma_0) \cap \Gamma_0'$ is finite. Suppose $\psi \in \mathrm{H}(B, A')$ and $\psi_1, \dots, \psi_r \in \mathrm{E}(A')$ satisfy $\psi(P) + \Sigma_i \psi_i(Q_i) = 0$. Then $\psi(P) \in \Gamma_0'$ and corollary 4.2 implies $\psi(P) \in \phi(\Gamma_0)$, thus $\psi(P)$ lies in the finite intersection $\phi(\Gamma_0) \cap \Gamma_0'$ and so $\psi(P) = 0$ by our assumptions on P. Therefore, since $Q_1, \dots, Q_r$ are almost free, we have $\{\psi_i(Q_i)\}_i = \{0\}$ and so $\{\psi(P), \psi_i(Q_i)\}_i = \{0\}$.

Suppose $\psi \in \mathrm{E}(B)$ and $\psi_1, \dots, \psi_r \in \mathrm{H}(A', B)$ satisfy $\psi(P) + \Sigma_i \psi_i(Q_i) = 0$. For each i, let $\psi_i' \in \mathrm{H}(B, A')$ be such that the kernel of ψ_i has finite index in $\ker(\psi_i' \psi_i)$ (cf. lemma 2.1), and consider the identity $\psi_i' \psi(P) + \Sigma_j \psi_i' \psi_j(Q_j) = 0$. As in the previous paragraph, $\psi_i' \psi(P) = 0$ and thus $\{\psi_i' \psi_j(Q_j)\}_j = \{0\}$ for every i. That is, $\psi_j(Q_j)$ lies in the kernel of ψ_i' for every i, j, and a fortiori for every $i = j$. In particular, since $\ker(\psi_i)$ has finite index in $\ker(\psi_i' \psi_i)$, $\psi_i(Q_i)$ is torsion. By our assumptions on $Q_1, \dots, Q_r$, we have $\{\psi_i(Q_i)\}_i = \{0\}$ and thus $\{\psi(P), \psi_i(Q_i)\}_i = \{0\}$. Therefore, $P, Q_1, \dots, Q_r$ are almost free as claimed. □

We suppose for the remainder of the section that $B = 0$ and thus $A = B' \subseteq A'$ and ϕ is the inclusion. Let $\{Q_1, \dots, Q_r\} \subset \Gamma'$ be a maximal subset of almost free points, and let $\Gamma_0' \subseteq \Gamma'$ be the finite-index submodule they generate (which we may suppose to be torsion free) and ℓ be a prime not dividing $[\Gamma' : \Gamma_0']$.

Suppose condition 1 fails and thus $\Gamma \cap \Gamma'$ has infinite index in Γ. Therefore the index of $\phi_*(\Gamma) \cap \Gamma'$ in $\phi_*(\Gamma)$ is infinite and lemma 3.6 implies there exists $P \in \phi_*(\Gamma)$ such that $P, Q_1, \dots, Q_r$ are almost free.

If $\mathfrak{p} \in S_{\ell,m}(P, Q_1, \dots, Q_r)$, then $\mathrm{ord}_\ell(\Gamma_\mathfrak{p}) \geq m$ and $\mathrm{ord}_\ell(\Gamma_\mathfrak{p}') = 0$, thus we have the following inequalities:

$$\nu_{\ell,\Gamma}(\mathfrak{p}) \geq \varepsilon_{\ell,\Gamma}(\mathfrak{p}) = \varepsilon_{\ell,\phi_*(\Gamma)}(\mathfrak{p}) \geq m \geq \nu_{\ell,\Gamma'}(\mathfrak{p}) = \varepsilon_{\ell,\Gamma'}(\mathfrak{p}) = 0.$$

In particular, if $\ell \gg 0$, then proposition 3.2 implies $S_{\ell,m}(P, Q_1, \dots, Q_r)$ has positive density for every $m \geq 0$, and thus 2, 3, and 4 fail.

Q.E.D.

References

[1] J. Demeyer and A. Perucca, *The constant of the support problem for abelian varieties*, arXiv:1008.3719.

[2] G. Faltings, *Finiteness Theorems for Abelian Varieties over Number Fields*, Arithmetic Geometry, Edited by G. Cornell and J. H. Silverman, Springer-Verlag, New York, 1986, 9–27.

[3] M. Hindry and J. Silverman, *Diophantine Geometry. An Introduction*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.

[4] A. Perucca, *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*, J. Number Theory **129** (2009), no. 2, 469–476.

[5] A. Perucca, *On the reduction of points on abelian varieties and tori*, Int. Math. Res. Notices **2011** (2011), no. 7, 293–308.

[6] Y. Zarhin, *Homomorphisms of abelian varieties over finite fields*, Higher-dimensional geometry over finite fields, Edited by D. Kaledin and Y. Tschinkel, IOS, Amsterdam, 2008, 315–343.

Chris Hall, University of Wyoming
E-mail: chall14@uwyo.edu

Antonella Perucca, Research Foundation - Flanders (FWO)
E-mail: antonellaperucca@gmail.com